

### **REMARKS**

Claims 1-25 were pending in the above-identified application when last examined. Claims 1-25 are presented for reconsideration and allowance.

#### **Claim Rejection under 35 U.S.C. § 103**

Claims 1-17 stand rejected under 35 U.S.C. 103(a) as being unpatentable over Droms et al. (U.S. Patent 7,143,435) in view of Donaldson (US Patent 7,249,175).

Applicant respectfully traverses. The currently pending claims are not obvious in view of the cited references for at least the reasons set forth below. Reexamination and reconsideration are requested.

#### **The Invention of Claim 1**

Claim 1 is independent and is printed as follows for convenience:

"A method of **developing an access control list**, comprising:

**developing an enhanced access control list including data related to at least one of user names, DNS names, Windows domain names, and physical addresses;**  
converting at least one of,

**user names into corresponding IP and physical addresses according to data in the enhanced access control list;**

DNS names into corresponding IP addresses according to data in the enhanced access control list; and

physical addresses into IP addresses according to data in the enhanced access control list; and

developing the access control list from each of the operations of converting."

(Claim 1, emphasis added)

At least the above highlighted features are not disclosed or suggested by Droms or Donaldson either individually or in combination and would not have been obvious to a person with ordinary skill in the art having the cited references before him.

**Droms et al.**

Droms does not teach or suggest a method of **developing an access control list**. Droms is not directed to a method of developing an access control list. Droms discloses a gateway with a standard access control list and a DHCPv6 server that stores information about auto-configured IPv6 addresses. (See, e.g., col.8, line 44-col. 9, line 27) For example:

**“According to the illustrated embodiment, the DHCPv6 server 113 registers auto-configured IPv6 addresses** in response to DHCP information request (INFORM) messages. The DHCPv6 server 113 performs the registration by storing a data structure herein called a map 114. Map 114 associates an IPv6 address supplied in the INFORM message by the host with authentication or authorization information, or both, supplied in the INFORM message by a DHCPv6 relay agent in an intermediate device connected to the host. Conventional DHCP does not require or suggest that the DHCPv6 server 113 obtain authentication or authorization information from a DHCP relay agent. Conventional DHCP does not require or suggest that the DHCPv6 server 113 store or use the map 114.

In addition, in some embodiments, the DHCPv6 server 113 also stores one or more data structures that associate other configuration information with authentication or authorization information, or both.”  
(Droms col. 8, lines 49-66, emphasis added)

**“The gateway maintains an access control list 146 of IP addresses in one or more data structures. Only a client operating on a host having an IP address included in the access control list 146 is allowed by the gateway 145 to exchange data packets over the Internet 150. If a request to access the Internet comes from a host with an address unknown to the gateway 145, the gateway 145 may request user identification information associated with that**

**address from the DHCP server host 112 based on information in the map 114. The gateway 145 also may obtain authorization information such as an access control list from the AAA server 132. The gateway 145 is one example of a network server in which the service provided depends on registering an auto-configured logical network address."**

(Droms col. 9, lines 14-27)

Droms does not teach or suggest **an enhanced access control list including data related to at least one of user names, DNS names, Windows domain names, and physical addresses**. Droms' gateway 145, which contains an access control list 146, relies on the registration of auto-registered IPv6 addresses in the DHCPv6 server 113 when a request is received by the gateway 145 from a host with an address not on the list of IP addresses in the access control list 146. Thus, Droms includes a traditional access control list containing IP addresses, but does not disclose an enhanced control list. There is no suggestion in Droms that an enhanced access control list is generated containing more information than a list of IP addresses. Rather, Droms discloses a standard access control list in a gateway and a data structure containing additional information in a separate DHCPv6 server. If Droms disclosed an enhanced control list, there would be no need for the gateway 145 to query the DHCPv6 server when an unknown IP address is detected. It is noted that DHCP servers typically do not control network access and do not contain access control lists, they merely assign network parameters such as IP addresses to other devices on the network. They are typically not used for security. Similarly, the data structure or map contained in Droms' DHCPv6 server is not an access control list or an enhanced control list. It does not contain a list of all devices authorized to access a network, and is not used to control access.

Droms does not teach or suggest converting **user names into corresponding IP and physical addresses according to data in the enhanced access control list**. Droms does not disclose what information about auto-registered IPv6 addresses is registered by the DHCPv6 server, specifying only "authentication or authorization

information". (See, e.g., col. 8, line 55) Droms therefore does not disclose converting user names and physical addresses into IP addresses, particularly according to data in an enhanced access control list.

### **Donaldson**

Donaldson does not teach or suggest converting **user names into corresponding IP and physical addresses according to data in the enhanced access control list**. Donaldson is not directed to a method of developing an access control list. Donaldson discloses a system and method for filtering undesirable e-mail with forged nonexistent sender addresses in real time without sending a message to that sender (See Abstract). Donaldson teaches that when a remote host attempts to send mail to a user at a local network, the remote host gets the name of the proxy server from the MX record, translates the name into an IP address (See, e.g., col. 13, lines 26-29). Donaldson does not teach or suggest converting user names into corresponding IP and physical addresses according to data in the enhanced access control list.

Applicant therefore believes that claim 1 is allowable over the cited references at least because neither Droms nor Donaldson either individually or in combination disclose an enhanced access control list, and converting information from the enhanced access control list to develop an access control list. Applicant respectfully requests reconsideration.

Dependent claims 2-8 depend ultimately upon independent claim 1 which is allowable over the cited art as discussed above. These dependent claims are likewise in condition for allowance at least because they depend on an allowable independent claim. Dependent claims 2-8 are also allowable, on further independent grounds, in that they recite particular features which, when combined with the elements of the independent claim, are also not disclosed or suggested in the cited references.

The Invention of Claim 9

Claim 9 is independent and is printed as follows for convenience:

"A method of controlling access of a user to a network including a plurality of hosts coupled together through a network switch, the method comprising:

**storing in the network switch an enhanced access control list containing data related to at least one of user names, DNS names, Windows domain names, and physical addresses;** and

generating a dynamic access control list from the enhanced access control list, the dynamic access control list containing a plurality of IP addresses that restrict access of the user to the network."

(Claim 9, emphasis added)

Applicant repeats the arguments for allowability set forth above with respect to claim 1, but specifically directed to the method set forth in claim 9. Droms does not disclose or suggest **storing in the network switch an enhanced access control list containing data related to at least one of user names, DNS names, Windows domain names, and physical addresses**. Droms' gateway contains a conventional access control list as discussed above, which relies on queries to a DHCPv6 server to handle queries from hosts with IP addresses not in the access control list. Droms' switch 102 does contain an authenticator 105 that stores "authentication and authorization data". The content of this information is unspecified except to indicate that it includes a user class. (See, e.g., col. 14, lines 43 and 67). The switch 102 does not contain an enhanced access control list from which a dynamic access control list is generated. Rather, the authenticator and a DHCP relay process in Droms' switch 102 communicate with an external authentication server (AAA server) in order to configure a DHCP server external to the switch 102. (See claim 29)

Applicant therefore believes that claim 9 is allowable over the cited references at least because neither Droms nor Donaldson either individually or in combination disclose **storing in the network switch an enhanced access control list containing data related to at least one of user names, DNS names, Windows domain names, and physical addresses**. Applicant respectfully requests reconsideration.

Dependent claims 10-17 depend upon independent claim 9 which is allowable over the cited art as discussed above. These dependent claims are likewise in condition for allowance at least because they depend on an allowable independent claim. Dependent claims 10-17 are also allowable, on further independent grounds, in that they recite particular features which, when combined with the elements of the independent claim, are also not disclosed or suggested in the cited references.

Claims 18-25 stand rejected under 35 U.S.C. 103(a) as being unpatentable over Droms et al. (U.S. Patent 7,143,435) in view of Fan et al. (US Patent 6,219,706).

Applicant respectfully traverses. The currently pending claims are not obvious in view of the cited references for at least the reasons set forth below. Reexamination and reconsideration are requested.

#### The Invention of Claim 18

Claim 18 is independent and is printed as follows for convenience:

"A network switching circuit, comprising:

a forwarding circuit operable to detect specific received packets and to provide the specific packets on a processor port, and further operable to receive packets on one of a plurality of ports including the processor port and to forward each received packet to a port corresponding to a destination address contained in the packet subject to access restrictions contained in a dynamic access control list;

a memory circuit coupled to the forwarding circuit, the memory circuit operable to store packets and **operable to store an enhanced access control list and a dynamic access control list**; and

a processor coupled to the forwarding circuit and to the memory circuit, the processor operable to define the specific packets detected by the forwarding circuit and **operable to process the specific packets stored in the memory circuit using the enhanced access control list to generate the dynamic access control list and store the dynamic access control list in the memory circuit**, and further operable to provide the specific packets to the processor port of the forwarding circuit after processing the packets."

(Claim 18, emphasis added)

Applicant repeats the arguments for allowability set forth above with respect to claim 1, but specifically directed to the network switching circuit set forth in claim 18. Droms does not disclose or suggest a memory circuit in a network switching circuit that is **operable to store an enhanced access control list and a dynamic access control list**. Droms also does not disclose or suggest a processor in a network switching circuit that processes **specific packets stored in the memory circuit using the enhanced access control list to generate the dynamic access control list**.

Applicant therefore believes that claim 18 is allowable over the cited references at least because neither Droms nor Fan either in individually or in combination disclose an enhanced access control list, and converting information from the enhanced access control list to develop a dynamic access control list. Applicant respectfully requests reconsideration.

Dependent claims 19-21 depend upon independent claim 18 which is allowable over the cited art as discussed above. These dependent claims are likewise in condition for allowance at least because they depend on an allowable independent claim. Dependent

claims 19-21 are also allowable, on further independent grounds, in that they recite particular features which, when combined with the elements of the independent claim, are also not disclosed or suggested in the cited references.

The Invention of Claim 22

Claim 22 is independent and is printed as follows for convenience:

"A computer network, comprising:

a network switch, including,

a forwarding circuit operable to detect specific received packets and to provide the specific packets on a processor port, and further operable to receive packets on one of a plurality of ports including the processor port and to forward each received packet to a port corresponding to a destination address contained in the packet subject to access restrictions contained in a dynamic access control list;

a memory circuit coupled to the forwarding circuit, the memory circuit **operable to store packets and operable to store an enhanced access control list and a dynamic access control list**; and

a processor coupled to the forwarding circuit and to the memory circuit, the processor operable to define the specific packets detected by the forwarding circuit and **operable to process the specific packets stored in the memory circuit using the enhanced access control list to generate the dynamic access control list and store the dynamic access control list in the memory circuit**, and further operable to provide the specific packets to the processor port of the forwarding circuit after processing the packets; and

a plurality of hosts, each host coupled to a respective port of the network switch."

(Claim 22, emphasis added)



Applicant repeats the arguments for allowability set forth above with respect to claim 1, but specifically directed to the computer network set forth in claim 22. Droms does not disclose or suggest a memory circuit **operable to store packets and operable to store an enhanced access control list and a dynamic access control list**. Droms also does not disclose or suggest a processor **operable to process the specific packets stored in the memory circuit using the enhanced access control list to generate the dynamic access control list and store the dynamic access control list in the memory circuit**.

Applicant therefore believes that claim 22 is allowable over the cited references at least because neither Droms nor Fan either individually or in combination disclose an enhanced access control list, and converting information from the enhanced access control list to develop a dynamic access control list. Applicant respectfully requests reconsideration.

Dependent claims 23-25 depend upon independent claim 22 which is allowable over the cited art as discussed above. These dependent claims are likewise in condition for allowance at least because they depend on an allowable independent claim. Dependent claims 23-25 are also allowable, on further independent grounds, in that they recite particular features which, when combined with the elements of the independent claim, are also not disclosed or suggested in the cited references.

In view of the above, all of the claims are believed to be in condition for allowance, and the Applicant respectfully requests that a timely Notice of Allowance be issued.

Respectfully submitted,  
KLAAS, LAW, O'MEARA & MALKIN, P.C.

By: /John Pessetto/  
John R. Pessetto, Esq.  
Registration No. 48,369  
1999 Broadway, Suite 2225  
Denver, CO 80202  
(303) 298-9888  
Fax: (303) 297-2266